A note on factorisation of division polynomials

D. Sadornil

Departamento of Matemáticas,U. Salamanca
Pza. de la Merced 1-4, 37008 Salamanca, Spain.
email: sadornil@usal.es

Abstract

In [2], Verdure gives the factorisation patterns of division polynomials of elliptic curves defined over a finite field. However, the result given there contains a mistake. In this paper, we correct it.

1 Introduction

Let $p > 3$ be a prime number and q a power of p. Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Thus, we can assume that E has equation $E : y^2 = x^3 + ax + b$.

The set of rational points on E, denoted by $E(\mathbb{F}_q)$, has group structure. If n is an integer, we denote by $E(\mathbb{F}_q)[n]$ (or $E[n]$ if the field is the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$) the rational points of order n. If n is relatively prime with p, $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Let $\psi_n(x)$ be the division polynomials of E (see [1]). As it is well known, the roots of the polynomial ψ_n are the abscissas of the n-torsion points, that is

$$P = (x, y) \in E[n] \Leftrightarrow \psi_n(x) = 0.$$

Hence, the factorisation patterns of these polynomial give information about the extension where the n-torsion points are defined.

The Frobenius endomorphism,

$$\begin{array}{rccc} \varphi : & E(\overline{\mathbb{F}_q}) & \to & E(\overline{\mathbb{F}_q}) \\ & (x, y) & \to & (x^q, y^q) \end{array}$$

characterizes the rationality of a point of the elliptic curve as follows

$$\forall P \in E(\overline{\mathbb{F}_q}),\ P \in E(\mathbb{F}_{q^n}) \Leftrightarrow \varphi^n(P) = P.$$

In the paper *Factorisation of division polynomials* (Proc. Japan Academy, Ser A. 80, no. 5, pp. 79-82), Verdure gives the degree and the number of factors of the division polynomial of an elliptic curve. However, the result present there contains a mistake. We correct it here.

2 Patterns of l-th division polynomials

Let l be an odd prime different from the characteristic of $\mathbb{F}_q$. We present here the factorisation patterns of division polynomial only when the l-torsion points generate different extension fields (the wrong result in [2]). If all l-torsion points are defined over the same extension field, the factorisation can be found in [2].

First of all, we fix the notation. Let f be a one variable polynomial over a field K of degree n. We say that the factorisation pattern of f is

$$((\alpha_1, n_1), \dots, (\alpha_d, n_d))$$

if f factorizes over K as

$$f = k \prod_{i=1}^{d} \prod_{j=1}^{n_i} P_{i,j}$$

with $P_{i,j}$ an irreducible polynomial of degree α_i.

The next result shows how the Frobenius endomorphism acts on $E[l]$ when the l-torsion points are not all defined over the same extension of $\mathbb{F}_q$.

Lemma 1 ([2]) *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let α be the degree of the minimal extension over which an l-torsion point is defined, l an odd prime not equal to the characteristic of $\mathbb{F}_q$. Assume that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Then there exist $\rho \in \mathbb{F}_l^*$ of order α and a basis P, Q of $E[l]$ over $\mathbb{F}_l$ in which the n-th power of the Frobenius endomorphism can be expressed, for all n, as:*

$$\begin{pmatrix} \rho^n & 0 \\ 0 & (\frac{q}{\rho})^n \end{pmatrix} \qquad \begin{pmatrix} \rho^n & n\rho^{n-1} \\ 0 & \rho^n \end{pmatrix}$$

if $\rho^2 \neq q$ or $\rho^2 = q$ respectively. The number ρ is uniquely defined by the above properties.

The previous result help us to determine the factorisation pattern of division polynomial $\psi_l(x)$ when its factors are not all of the same degree. The next proposition solves the mistake, in the function $i(x, y)$, made in [2].

Proposition 2 *Let E be an elliptic curve defined over $\mathbb{F}_q$. Let α be the degree of the minimal extension over which E has a non-zero l-torsion point. Assume that $E[l] \not\subset E(\mathbb{F}_{q^\alpha})$. Let $\rho \in \mathbb{F}_l^*$ be as defined in Lemma 1. Let β be the order of q/ρ in $\mathbb{F}_l^*$. Then the pattern of the division polynomial ψ_l is:*

$$((h(\alpha), \tfrac{l-1}{2h(\alpha)}), (h(\beta), \tfrac{l-1}{2h(\beta)}), (i(\alpha,\beta), \tfrac{(l-1)^2}{2i(\alpha,\beta)})) \qquad \text{if } q \neq \rho^2,$$

$$((h(\alpha), \tfrac{l-1}{2h(\alpha)}), (h(\alpha)l, \tfrac{l-1}{2h(\alpha)})) \qquad \text{if } q = \rho^2,$$

with

$$h(x) = \begin{cases} x, & x \text{ odd}, \\ \frac{x}{2} & x \text{ even}, \end{cases},$$

and

$$i(x, y) = \begin{cases} \frac{lcm(x,y)}{2}, & x, y \text{ even and } \upsilon_2(x) = \upsilon_2(y), \\ lcm(x, y), & \text{otherwise}. \end{cases}$$

Remmark 3 *Verdure gives the function $i(x,y) = \ lcm(x,y)/2$ when x and y are both even.*

Proof.

We follow the proof given in [2] except for the wrong cases.

Let I be an irreducible factor $\psi_l(x)$ of degree d, and P a point of l-torsion corresponding to one of its roots, then d is the minimum positive integer n such that $\varphi^n(P) = \pm P$. Let (P,Q) be a basis of $E[l]$ as in Lemma 1. We distinguish the cases $q \neq \rho^2$ and $q = \ \rho^2$.

i) Suppose that $q \neq \rho^2$. If R is an l-torsion point which is a non-zero multiple of P (or Q), we have that the minimum n such that $\varphi^n(R) = \pm R$ is $n = h(\alpha)$ (or $h(\beta)$). Notice that, $\varphi^n(R) = -R$ if and only if α (or β) is even, and hence $n = \alpha/2$ (or $\beta/2$).

   Finally, let R be any non-zero l-torsion point not of the previous form, then $R = k(P + jQ)$ with $1 \leq j,k \leq l-1$. So, $\varphi^n(R) = k(\varphi^n(P) + j\varphi^n(Q))$. The subgroup generated by R ($\langle R \rangle$) is rational over $\mathbb{F}_{q^n}$ if and only if $\varphi^n(R) = \pm R$. The minimum extension where $\langle R \rangle$ is defined is $\mathbb{F}_{q^n}$, with n minimum such that $\varphi^n(R) = \pm R$.

   It is easy to prove that $\varphi^n(R) = R$ if and only if $\varphi^n(P) = P$ and $\varphi^n(Q) = Q$. Hence $lcm(\alpha,\beta) \mid \ n$ and $n = lcm(\alpha,\beta)$ is the minimum.

   On the other hand, $\varphi^n(R) = -R$, if and only if $\varphi^n(P) = -P$ and $\varphi^n(Q) = -Q$. This is only possible when α and β are both even. Moreover, $lcm(\alpha/2,\beta/2) \mid n$ and α or β not divides $lcm(\alpha/2,\beta/2)$ (if, for example, $\alpha \mid lcm(\alpha/2,\beta/2)$, then $\varphi^n(P) = P$). On the other hand, $\alpha/2$ and $\beta/2$ have the same parity, otherwise, for example, if $\alpha/2$ is even and $\beta/2$ odd then $lcm(\alpha/2,\beta/2) = lcm(\alpha/2,\beta)$ and β divides $lcm(\alpha/2,\beta/2)$ which is a contradiction. If $\upsilon_2(\alpha) = \upsilon_2(\beta)$, then $n = lcm(\alpha/2,\beta/2)$ is the minimum integer such that $\varphi^n(P) = -P$ and $\varphi^n(Q) = -Q$. Otherwise, if both valuations are not equal, $lcm(\alpha/2,\beta/2)$ is divisible by α if $\upsilon_2(\alpha) < \upsilon_2(\beta)$ (by β if $\upsilon_2(\alpha) > \upsilon_2(\beta)$) which contradicts $\varphi^n(R) = -R$.

   Counting the number of points of each type, namely $l-1$, $l-1$ and $(l-1)^2$, we have the number of factors of each type.

ii) Suppose that $q = \rho^2$. A point which is a non-zero multiple of P leads to factors of degree α or $\alpha/2$ as before. If R is not a multiple of P, then in order to have $\varphi^n(R) = \pm R$, we have that $\rho^n = \pm 1$ and $n\rho^{n-1} = 0$. Then, depending on the parity of α, we have $n = lcm(\alpha, l)$ or $n = lcm(\alpha/2, l)$. Finally, since $\alpha \mid l-1$, it is relatively prime to l. Therefore, these values are $h(\alpha)l$.

□

Example 4 *Consider the elliptic curve $y^2 = x^3 + 3x + 6$ over $\mathbb{F}_{17}$ and take $l = 5$. Then $\alpha = 2$ and $\beta = 4$. According to [2], the pattern of $\psi_5(x)$ should be $((1,2),(2,1),(2,4))$, but in fact it is $((1,2),(2,1),(4,2))$.*

I am grateful to the referee, for this careful review and his suggestion at the preliminar version.

References

[1] J.H. Silverman. The arithmetic of elliptic curves. GTM 106. Springer-Verlag, New-York. 1986.

[2] H. Verdure. Factorisation of division polynomials. Proc. Japan Academy, Ser A. 80, no. 5, pp. 79-82. 2004.